The Honorable John C. Coughenour

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

REBECCA COUSINEAU, individually on her own behalf and on behalf of all others similarly situated,

Plaintiff,

v.

MICROSOFT CORPORATION, a Delaware corporation,

Defendant.

Case No. 2:11-cv-01438-JCC

PLAINTIFF'S RESPONSE IN OPPOSITION TO MICROSOFT'S MOTION FOR SUMMARY JUDGMENT

NOTE ON MOTION CALENDAR: January 17, 2014

ORAL ARGUMENT REQUESTED

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

TABLE OF CONTENTS

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

TABLE OF AUTHORITIES

United States Supreme Court Cases

United States Court of Appeals Cases

United States District Court Cases

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

United States Statutes and Rules of Procedure

Legislative History Materials and Secondary Sources

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

I. INTRODUCTION[1]

Defendant Microsoft Corp. ("Microsoft"), one of the world's largest technology companies, programmed its smartphone Camera application to let users choose whether they wanted Microsoft to have access to data about their current physical location. The choice, however, was illusory—Microsoft also programmed its software to ignore each user's response, access location information no matter what, and use that information to improve its suite of location services and close the gap with its competition in the smartphone marketplace.

In 2010, Plaintiff Rebecca Cousineau ("Cousineau") used a Samsung phone equipped with Microsoft's Windows Mobile 7 ("WM7") operating system. When she first opened the phone's pre-installed Camera application, she declined to "share" her location information with Microsoft. Microsoft ignored her choice and accessed her location information anyway. And because Cousineau's WM7 phone was an integral and functional component of the system through which Microsoft aggressively "crowd sourced" and collected "Beacon" data—i.e., identifying information transmitted by cellular towers and WiFi routers, which was later stored and processed in its database (called "Orion")—Microsoft's unauthorized access of Cousineau's phone's memory violated the Stored Communications Act, 18 U.S.C. § 2701 ("SCA").

In its motion, Microsoft rehashes many attacks previewed in its opposition to Cousineau's motion for class certification, reasserting that Cousineau has shifted her theory of liability from a claim based on the transmission of data to Microsoft's servers to one based on Microsoft's improper access to the location information stored on the random access memory ("RAM") in her phone. Cousineau has already explained why Microsoft's characterizations are wrong, (*see* Dkt. 97 at 7 – 8), but it bears repeating that throughout this case, Cousineau has

[1] Cousineau is generally not re-filing material previously submitted in her class certification briefing. (*See* Dkts. 71, 72, 89.) For the Court's convenience, however, Cousineau will include in the courtesy copies mailed to the Court factual material cited in this Response but previously filed. Factual materials, including excerpts, not previously filed are attached to the Declaration of Rafey S. Balabanian ("Balabanian Decl."), submitted concurrently herewith. All references to Exhibits (e.g., "Ex. A"), refer to exhibits described in and attached to the Balabanian Declaration. References to specific page numbers from Microsoft's document production refer to the unique Bates Number designations as marked by Microsoft (e.g., page "531" refers to the page marked MS-COUS_00000531).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

maintained a singular theory of liability under the SCA: Microsoft violated the SCA by exceeding the scope of its authority to access the RAM in Cousineau's WM7 phone, and then obtaining communications including location information it was specifically denied access to.

Now, Microsoft brings two types of arguments. First, it says that the SCA doesn't apply in this case. It says that a smartphone like Cousineau's WM7 phone, *cannot* be a facility through which an electronic communications service ("ECS") is provided, relying on a line of case law addressing defendants' unconsented access to text messages and emails. It also argues that the communications it accessed—the Beacon and location information stored in the RAM on Cousineau's phone—were not held in "electronic storage" as required by the SCA. Both arguments fail. Even if smartphones are not facilities through which email or text message services are provided, this Court has already recognized the technological possibility that smartphones *can* be ECS facilities depending on the configuration of the ECS at issue. And here they are, because WM7 phones served an essential function in the system that Microsoft developed to (i) capture data transmitted by Beacons, (ii) attribute location information to unrecognized Beacons, (iii) send the foregoing data to Orion for processing, and (iv) transmit location information from Orion to users' WM7 phones. Likewise, Microsoft's claim that location information stored in a phone's RAM is not in "electronic storage" fails because Congress specifically stated that data in RAM is in "electronic storage," and because Microsoft accessed Cousineau's RAM to obtain location information that was temporarily stored in pendency of transit elsewhere.

Second, Microsoft claims that even if the SCA applies to the facts, Microsoft did not violate it. It says that it cannot be liable for conduct that took place within Cousineau's phone, and that because Cousineau allowed Microsoft to access her RAM-stored location information in *some* instances, she cannot sue based on Microsoft's "misuse" of that same information. This defense fails as well. Because *Microsoft* created a platform where WM7 users could selectively allow or deny applications' access to their location information, *it* is liable for its own software's

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

actions. Likewise, that Microsoft was authorized to access Cousineau's RAM-based location information in *some* instances (e.g., when and where she approved access for other applications) does not mean that it was permitted access location information when and where it was specifically prohibited from doing so—a fact driven home by the SCA's express prohibition on "exceeding the scope of authorized access" to an ECS facility. *See* 18 U.S.C. § 2701(a)(1).

As explained more fully below, because the SCA applies to the facts at hand and prohibited Microsoft's conduct, the Court should deny Microsoft's motion.

II. BACKGROUND

A. WM7-equipped phones allow users to send and receive communications containing location information.

Microsoft equipped WM7 phones with software (the "Location Framework") that enabled users to run applications that do things like perform location-based searches, provide driving directions, or let users "geo-tag" digital photographs. (*See* Dkt. 69 at 8 – 11.) A key part of WM7's Location Framework platform is its reliance on unique identifying data transmitted by WiFi routers and cell towers (called "Beacons" by Microsoft), that, as part of Microsoft's ongoing efforts to populate its Orion database with "crowd sourced" Beacon data from WM7 users, (i) is coupled with locational data and then (ii) used to resolve WM7 devices' locations faster than through a GPS location fix. (Dkt 91 at ¶ 8; *see also* Dkt. 64-2 at 6.) Location Framework then uses data from one or more components (GPS, Beacons, and/or Orion) to resolve a phone's location, depending on the type of request received from an application. (Expert Witness Report of Craig Snead, Dkt. 72-4 ("Snead Rpt.") at 13 – 16.)

Given the sensitive nature of information concerning a user's physical location, Microsoft only allows "authorized" applications to make calls to Location Framework. (*See* Location Service Functional Specification, Ex. A, at 531.) Microsoft vets third-party (i.e., non-Microsoft) applications (e.g., the Facebook application) to ensure that the software has a legitimate need to access location information, and additionally requires the software's developer to program the

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

application to obtain and honor user consent before gaining access. (*See* Ex. A, at 532.) By contrast, applications developed by Microsoft (e.g., Camera) are "pre-approved" and automatically "trust[ed] that they do not use location unless consent is given by the user." (*See* Location UX Functional Specification, Ex. B, at 1307.)

Authorized applications can initiate calls to Location Framework with instructions to return location information. (*See* Snead Rpt. at 13 – 15.) The application's developers may choose from various types of calls to specify which method (or methods) for Location Framework to use when attempting to resolve the phone's location (i.e., GPS, Beacons, and/or Orion). (*Id*.) Microsoft programmed Camera's calls to Location Framework to "resolve location using *both* GPS and available Beacons," (Dkt. 91 at ¶ 8), resulting in the following sequence of operations.

First, Location Framework attempts to resolve the phone's location using Beacons. This process starts with Location Framework accessing Beacon signals "visible" to (or "seen" by) the phone. (*See* Snead Rpt. at 14.) The access is facilitated by hardware components on the WM7 device ("Background Scanners"), which (i) recurrently scan for signals from nearby Beacons and (ii) temporarily store such seen Beacon data independent of Location Framework. (*See* Location WiFi Provider Developer Design Specification, Ex. C, at 651; WiFi Location RIL Provider Developer Design Specification, Ex. D, at 716, 721.) Next, Location Framework compares the "seen"[2] Beacons with certain "tiled" Beacon data[3] held in the phone's RAM. (Dkt. 91 at 5 – 7, 11.) If "seen" Beacons match up with RAM-stored tile data (i.e., data about the location of

---

[2] Regarding this "seen" Beacon data, Location Framework first looks to see if the phone's Background Scanners have recently (within the past 60 seconds) received data from visible Beacons. (Ex. C, at 652.) If they have, that Beacon data is used by Location Framework. (*Id.*) Otherwise, Location Framework activates the Background Scanners to capture new signal data from visible Beacons. (*Id.* at 651 – 52.)

[3] Tiled data—or "tiles"—are a collection of Beacons for which approximate latitude and longitude are known, and which exist within a bounded geographic area. (Dkt. 91 at 5.) While WM7 stores tiles in both RAM and flash memory, it continuously shuffles tile storage locations (i.e., from flash to RAM) to ensure that the tile containing the device's likely location is stored in RAM. (*Id.* at 6 – 7.) As such, the RAM-stored tile data typically represents the most current approximation of the location for the device (i.e., as within the particular geographic boundaries of the then-RAM-stored tile).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

Beacons proximate to the user's location), then Location Framework returns the phone's resolved location back to Camera. (*Id.*) If, on the other hand, the RAM-stored tiles do not contain information about "seen" Beacons, then Location Framework follows a different process where it: (i) initiates a call to Orion (Microsoft's crowd-sourced database of Beacon location information, (Dkt. 91 at ¶ 9)), for new/refreshed tile data matching Beacons visible to the device; (ii) attempts to resolve location using additional tile data stored in flash memory (as opposed to RAM), and, if no matching data held in flash memory is found; (iii) waits for Orion to transmit additional tile data to the phone. (Snead Rpt. at 14 – 15.) If the newly received tile data contains location information for the visible Beacons after steps (ii) or (iii), then the phone's location will be returned to the requesting application. (*Id.*)

Second, Location Framework runs a separate and more time-intensive request that attempts to resolve the phone's location using GPS signals. (Dkt. 91 at ¶ 8.) All GPS events involve the WM7 phone receiving location information from orbiting GPS satellites. (Dkt. 91 at 4.) If GPS resolution process is successful, Location Framework sends the resolved location to the requesting application, while also caching the data for later transmission to Orion as part of Microsoft's "crowd sourcing" efforts. (Snead Rpt. at 15.) Relevant to issues driving this case, Microsoft engineers were informed that those "crowd sourcing" efforts were imperative.[4]

In any event, the Camera calls to Location Framework *always* involved first accessing a user's RAM to obtain the most recent, temporarily stored Beacon data. (Snead Rpt. at 14.)

[4] In summary, "crowd sourcing" is accomplished "when location is established through GPS [and] information about Beacons visible to the mobile device are collected and temporarily stored in association with the user's current geocoordinates." (*See* Wi-Fi/Cell Location Resolution and Caching Tiling Design Document, Ex. E, at 674.) This data is typically then later sent to Orion in batches. (*Id.* at 678; Location Crowd Sourcing Functional Specification, Ex. F, at 703 – 05.) Once received by Microsoft's servers, "previously unknown Beacons—meaning Beacons . . . with unique identifiers not recognized by Orion—are added to the Orion database and assigned geocoordinates." (Snead Rpt. at 9.) There is no dispute that Microsoft was highly motivated to crowd source data and did so aggressively, as crowd sourcing was both "one of the objectives of the Windows Phone Division, [i.e.] to ensure [Microsoft] had a good positioning service," (*See* Dep. Tr. of R. 30(b)(6) Designee Sandeep Deo, Dkt. 72-15, at 99:22 – 100:16), and viewed by Microsoft as a "competitive differentiator" for the product. (Ex. A, at 532 – 33; Dep. Tr. of R. 30(b)(6) Designee Cristina Del Amo Casado, Dkt. 72-16, at 182:4 – 183:25.) Whether that desire to aggressively crowd source data led to intentional design decisions to crowd source Beacon information even if a user opted out of "improving Microsoft's location services" will be a key merits issue.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

B. Microsoft programmed its Camera application to access users' RAM-stored Beacon location information irrespective of a user's consent.

Microsoft included the Camera application with WM7. The Camera's location functionality enabled (i) users to "tag" photos and videos with their locations and (ii) Microsoft to collect Beacon data as a part of its crowd sourcing efforts. Microsoft programmed Camera so that when the user first ran the application, a consent prompt displayed the following:

> **Allow the camera to use your location?**
>
> Sharing this information will add a location tag to your pictures so you can see where your pictures were taken. This information also helps us provide you with improved location services. We won't use the information to identify or contact you.

(Dkt. 65 at ¶ 4.) Users were given two options: "allow" or "cancel."[5] (*Id*.) Despite the privacy expectation created by these options, Microsoft designed Camera to call Location Framework and resolve the phone's location *every* time Camera was opened—including the first time—regardless of the user's choice. (*See* Dkt. 69 at 12:4 – 6.) And as detailed above, Location Framework *always* accessed the phone's RAM for Beacon data. (*Id.* at 12:9 – 13.)

C. Rebecca Cousineau used her WM7 phone to send and receive communications containing location information, and Microsoft accessed those communications stored in her phone's RAM without consent.

Rebecca Cousineau's WM7 experience began in June 2011, when she began using a WM7-equipped Samsung smartphone. (Dkt. 64 at ¶ 31.) Like all other WM7 phones, Cousineau's Samsung allowed her to send and receive electronic communications, including Beacon and other location information. (*Id.* at ¶ 32.) Cousineau intentionally used her phone's location functionality on several occasions, including when "checking in" using her Facebook application, or looking up driving directions with the phone's Maps applications. (*See* Dkt. 69 at

[5] The "allow or cancel" consent choice would then be stored on the phone and the user would not be asked for his/her preference again. (Snead Rpt. at 8 – 10.) If, as a third "option," the user closed the consent dialog box without making a choice, it would be "popped" each time the Camera was opened until a choice was made. (Dep. Tr. of R. 30(b)(6) Designee Adam Lydick ("Lydick Tr."), Ex. G, at 75:23 – 77:19.) But just as the 'allow or cancel' choice had no effect on Microsoft's choice to go forward with accessing location information (i.e., it would do it regardless), closing the dialog box likewise had no effect—as Camera would call Location Framework and request the phone's physical location the moment it was opened (even for the very first time and even if the consent dialog box was still displayed as a user was deciding which choice to make). (*Id.* at 23:19 – 30:13.)

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

24:8 – 21.) Each time, "seen" Beacon signals received by her phone were accessed and Location Framework's resolution processes were executed. (Snead Rpt. 13 – 15.)

Cousineau also used her phone's Camera application, often to document eviction proceedings in connection with her job. (*See* Mar. 13, 2013 Dep. Tr. of Rebecca Cousineau ("Cousineau 3/13 Tr."), Dkt. 71-23 at 34:24 – 36:7, 62:21 – 63:5, 71:15 – 71:20.) When she first opened Camera, Microsoft asked for permission to access her phone's location information (for "geo-tagging" and crowd sourcing purposes). (Snead Rpt. at 7 – 8.) And although Cousineau granted other applications authorization for such access (e.g., when and where she used Facebook or Maps applications), she explicitly denied Microsoft authorization access to this data when and where she used the Camera. (*See* Dkt. 69 at 24:15 – 17.)

Thus, when Cousineau used Facebook's "check-in" feature, for example, Microsoft (through Location Framework) had permission to access the phone's RAM *at that time* to seek the location information *then* in temporary storage. But on other occasions, including when Cousineau used Camera, Microsoft lacked such authority to access location information then in RAM. That distinction (i.e., choosing when and where Microsoft would, through WM7, resolve her location) was meaningful to Cousineau—while she didn't mind, for example, authorizing access to her location when eating at a restaurant and "checking in" with Facebook, she didn't consent to Microsoft resolving her location while using Camera to take pictures for her employer. (Cousineau 3/13 Tr., at 47:22 – 49:4; Dkt. 71-26, at ¶¶ 3 – 7.)

III. ARGUMENT

Under Federal Rule of Civil Procedure 56, "summary judgment is appropriate where there is 'no genuine issue as to any material fact' and the moving party is 'entitled to a judgment as a matter of law.'" *Alabama v. North Carolina*, 560 U.S. 330, 344 (2010) (quoting Fed. R. Civ. P. 56(c)). In deciding a motion for summary judgment, "[t]he evidence of the non-movant is to be believed, and all justifiable inferences are to be drawn in [her] favor." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986) (citing *Adickes v. S.H. Kress & Co.*, 398 U.S. 144, 158 –

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

59 (1970)). As detailed more fully below, Microsoft's motion rests on flawed interpretations of both the SCA and the material facts. Accordingly, its motion should be denied.

A. Microsoft's trespassory access to the Beacon location information stored on the RAM of Cousineau's phone falls within the purview of the SCA.

Two of Microsoft's arguments challenge the SCA's applicability to its conduct. First, Microsoft contends that the SCA does not apply because smartphones cannot be "facilities" through which electronic communications services are provided. Second, Microsoft argues that the RAM-stored Beacon location information it accessed was not in "electronic storage," and therefore did not fall within the SCA's purview.

Microsoft's sidestepping efforts fail. Cousineau's WM7 phone is a facility through which an ECS is provided because it was a necessary and functional *component* of Microsoft's location resolution service (an ECS involving, *inter alia*, communications between WM7 devices and Microsoft's Orion database), rather than a mere *recipient* of data from an ECS. Likewise, the Beacon location information improperly accessed by Microsoft was in "electronic storage" because it was in RAM, which Congress recognized as a type of electronic storage when it passed the SCA. The SCA governs the conduct. Microsoft's position is untenable.

1. Cousineau's WM7 phone is a facility through which an ECS is provided because that ECS depends on her phone to fully function.

Relying on a gloss of its selected case law, Microsoft contends that smartphones cannot be facilities through which electronic communications services are provided, and asserts that the WM7 device only "receive[s]" data as a "'client' for location services provided by the GPS satellites and Orion." (Def. Mot. at 19 – 20 (citing Dkt. 91 at ¶¶ 8, 9).) But a closer read of the SCA and available case law—along with an honest assessment of the facts surrounding the design of WM7 and operation of Microsoft's Location Framework software—shows that Cousineau's WM7 phone is a facility through which an ECS is provided. As designed, the phone is an integral part of Microsoft's location resolution communications system, without which Beacon-generated communications (the backbone of WM7's and Microsoft's location services)

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

could not enter the system, be tagged with locational data, or eventually be transmitted to Orion.

The SCA prohibits any person from "intentionally exceed[ing] an authorization to access [a facility through which an ECS is provided]." 18 U.S.C. § 2701(a). The Act doesn't define "facility," but does incorporate a definition of "electronic communication service"—i.e., "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). "Electronic communications," in turn, are broadly defined to include "*any* transfer of signs, signals, writing, sounds, data, or intelligence *of any nature* transmitted in whole or in party by an electromagnetic, photoelectronic or photooptical system that affects interstate commerce."[6] 18 U.S.C. § 2510(12) (emphasis added).

Here, WM7 phones satisfy each element necessary to show they are facilities through which electronic communications services are provided. First, Microsoft does not contest that WM7 phones contain **electronic communications** in the form of Beacon location information—e.g., WiFi router and cell tower identifiers, often coupled with locational data, transmitted to and from WM7 phones by wireless and cellular systems, and within the phone on wires and circuits. (*See generally* Ex. D.) The Beacon location information—as it is transmitted to, from, and within the phone—constitutes a "transfer of . . . data . . . in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce," and is therefore an electronic communication. 18 U.S.C. § 2510(12); *see Joffe v. Google, Inc.*, No. 11-17483, 2013 WL 6905957 (9th Cir. Dec. 27, 2013) (finding payload data, including router MAC addresses and SSIDs, transmitted by WiFi signal to be non-radio "electronic communications" within the meaning of § 2510); *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003) (noting that § 2510 "adopts a 'broad, functional' definition of an electronic communication) (quoting *Brown v. Waddell*, 50 F.3d 285, 289 (4th Cir. 1995)); *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 980 n.30 (C.D. Cal. 2010) ("As is clear, data are

[6] The definition of "electronic communication" includes four exceptions, none of which are relevant here. *See* 18 U.S.C. §§ 2510(12)(A) – (D).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

but one of several items that constitute communications.").

Next, each WM7 device houses and plays a necessary and functional part in several **electronic communications services** through which the above-referenced electronic communications are transmitted—including, most important to this case, the Location Framework/Orion ECS. As Microsoft concedes, the Location Framework/Orion ECS allows WM7 devices to send Beacon and locational data to Microsoft's Orion database, and also allows WM7 devices to receive tile data from the Orion database. (*See* Def. Mot. at 19 ("Here, the ECS involves the transmission of beacon data from Ms. Cousineau's Samsung phone, running Windows Phone 7, to the Orion service, and the return of location inference data from Orion to the phone."); *see also* Snead Rpt. at 8 – 9, 14 – 15.) Each of these transmissions involves electronic communications in the form of Beacon location information, and thus, as recognized by Microsoft, the phone hosts a "service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15); *see also Crispin*, 717 F. Supp. 2d at 982 n. 35 (recognizing that services which "enable communication" or "provide an electronic venue to communicate" are electronic communications services).

Finally, the SCA's "**facility-provision**" requirement is also met. Microsoft engineered the Location Framework/Orion ECS to rely on: (i) Beacons wirelessly broadcasting uniquely identifying information to its users' mobile devices (i.e., those "visible" Beacons that are "seen" by WM7 phones), (ii) WM7 capturing that "seen" Beacon data through WiFi and cellular hardware components, (iii) Location Framework comparing visible Beacon data to tile data stored in RAM, (iv) Location Framework requesting relevant tile data from Orion, (v) WM7 devices associating GPS coordinates to unrecognized visible Beacons, and (vi) WM7 devices sending unrecognized visible Beacons and their associated locations to Orion. (Dkt. 91 at 4 – 10.) In this system, the WM7 devices play an essential pass-through role by, for example, associating a location to received "seen" Beacon data, and then by passing the paired information to Microsoft. (*Id.*) And in this system, there are multiple points of ECS provision: **WM7 users**

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

are provided with *access* to the ECS by permitting applications (like Camera) to tap into and use their phone's Location Framework for different purposes; **Microsoft** is provided with *access* to the ECS through Orion, where crowd sourced data can be tiled and re-transmitted to other WM7 devices. (Dkt. 38 at 12 (recognizing that geolocation services could "both [be] provided by Microsoft in its installation of [WM7] on a phone *and* supported by its servers.") Stated simply, through the Location Framework/Orion ECS, Cousineau's WM7 phone enabled the sending and receiving of Beacon location information, (*see* Def. Mot. at 19 (acknowledging that phones sent Beacon data to Orion database, and Orion returned related and additional data)), and thereby "promote[d] the ease of [] action[s], operation[s], transaction[s] or course[s] of conduct," making it a facility through which those electronic communications services are provided. (Dkt. 38 at 11 (quoting Webster's Third New International Dictionary 812 (3d ed. 2002)).)

Rather than address these facts—that show the indispensable and functional role WM7 phones played in the Location Framework/Orion ECS—Microsoft contends that the case law establishes that (i) a personal computer or smartphone *cannot* constitute a facility through which an ECS is provided and (ii) recognizes a difference between devices that allow users to access, versus those that provide, an ECS. (*See* Def. Mot. at 19 – 20 (citing *Garcia v. City of Laredo*, 702 F.3d 788, 793 (5th Cir. 2012), *cert. denied*, 133 S. Ct. 2859 (2013)); *Shefts v. Petraki*s, No. 10-cv-1104, 2013 WL 489610, at *4 (C.D. Ill. Feb. 8, 2013); *Lazette v. Kulmatycki*, No. 12-cv-2416, 2013 WL 2455937, *5 (N.D. Ohio 2013); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1058 (N.D. Cal. 2012).) Neither contention succeeds, as each is based on an overgeneralization of the law. To start, nothing in the SCA's text or legislative history evinces any intent to preclude computers (or with them, smartphones) from being considered "facilities," and this Court, along with others, has already rejected such a categorical distinction. (*See* Dkt. 38 at 10 – 11 (citing *Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001); *United States v. Park*, No. CR 05-375, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007)); *see also* Def. Mot. at 22 (citing authorities recognizing the possibility of computers as ECS

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

facilities).)[7]

And, here, Microsoft's distinction between phones as points of user access rather than points of ECS provision actually illustrates why, under the facts of this case, Cousineau's WM7 phone is a facility *for the purposes of the ECS at issue*. In each case cited by Microsoft, the computer or phone evaluated was merely a way for the user to view or access a communication that had reached its end point—making the subject computer/phone external to the ECS itself. *See*, *e.g.*, *see Lazette*, 2013 WL 2455937, at *5 (smartphone not a facility through which email service was provided); *Garcia*, 702 F.3d at 793 (5th Cir. 2012) (cellular phone not a facility through which text message service was provided). In those examples, if the subject computer/phone was damaged or removed from the scenario entirely, the transmission at issue would still be complete—because the email would still reside with the email server (i.e., the point of ECS provision) even if it was never accessed by the particular computer/phone. *See Lazette*, 2013 WL 2455937, at *5. Or the text message would still reside with the provider of the relevant text messaging service (i.e., the point of ECS provision) even if that service was never accessed by the user's phone. *See, e.g., Shefts*, 2013 WL 489610, at *4; *Garcia*, 702 F.3d 788 at 793. Thus, in both circumstances, the destruction of the computer/phone would only limit the end user's ability to *view* the communication, a problem that could be remedied by using a different access device.

Here, in contrast, it's simply not possible to remove any given WM7 device without severing the Location Framework/Orion ECS. That's because without the WM7 device, the ECS would fail: the communications at issue (i.e., Beacon and location information collected and/or

---

[7] Microsoft additionally asserts that if the case law allowed for a computer or smartphone to count as a facility, it would only be where it provided server-like functions. (Def. Mot. at 22.) Here, Cousineau's WM7 phone (and more specifically, its RAM) *did* perform server-like functionality. It received Beacon data and location information, and acted as an intermediary in the transfer of that data to its ultimate destination (e.g., either to Orion or an application like Camera). (*See* Ex E.) Thus, Cousineau's WM7 phone operated in a server-like capacity, and, by Microsoft's own standard, is a facility through which an electronic communications service was provided. *See In re DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 501 (S.D.N.Y. 2001) (explaining that servers facilitate sending and receiving of communications).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

received by an individual WM7 phone and temporarily stored in its RAM) would *never* flow to Orion (i.e., via crowd sourcing) and tiled Beacon data could not flow to and/or be used by Location Framework on particular devices. (*See* Ex. F, at 693 ("Long term, crowd sourcing is the primary way that Orion collects the position of cell towers and WIFI beacons . . . most [priority one and priority two] markets must be boot strapped by WM7 devices in the field.").) And, of course, there's no option of using a different access point to tap into the system (in contrast to cases where an email or text message *could* be so-accessed from other points), because the functionality of the Location Framework/Orion ECS depends on comparisons between RAM-stored observations of "seen" Beacons and temporarily-held tiled Beacon data. (*Id.* at 692) Thus, by its design, Cousineau's WM7 phone (along with its RAM) is necessary to the provision of the Location Framework/Orion ECS and "'promotes the ease' of actions such as navigating from place to place, sharing information with others, and capturing images," (*see* Dkt. 38 at 11), making it a facility through which electronic communication services were and are provided.

Likewise, although Microsoft contends that "Orion provides ECS to the Windows Phone 7 device—not vice versa," (Def. Mot. at 19), it provides no support for that point (even though, by its own admission, both the WM7 devices and Orion both send and receive Beacon location information), and goes so far as to misrepresent the nature of the service and the WM7 device's role therein. True enough, Orion can provide a WM7 device with, upon request, tiled Beacon data. (Dkt 91 at ¶ 9.) But the process works the other way as well. Orion does not blindly send tile data to phones—rather, it relies on communications sent by WM7 devices via Location Framework (i.e., those identifying Beacons presently "seen" by the device) before determining which tile data to return. (*Id.*) And as described above, the function of the entire ECS relies upon crowd sourced (WM7-to-Orion) communications, which occur as WM7 phones (i) encounter previously unknown Beacons, (ii) are able to resolve their locations, and (iii) transmit that localized Beacon data to Orion in order to "improve[Microsoft's] location services"—where in fact WM7 devices *provide* location services to Orion/Microsoft. (*See* Snead Rpt. at 8 – 9, 14 –

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

15.) Thus, *both* the phone and the Orion server, along with the other necessary and contributing hardware along the way, function as facilities through which an ECS is provided to a user thereof—in this case, both (i) the WM7 phone user seeking to use location functionality and (ii) Microsoft seeking to benefit from crowd sourced Beacon data. (*Cf.* Dkt. 38 at 12 ("The language Congress chose, however, does not require only one point of ECS provision as Microsoft suggests. None of the facts Microsoft presents preclude the Court from finding that geolocation services are both provided by Microsoft in its installation of [WM7] on a phone *and* supported by its servers.").)[8]

In the end, and as the Court noted in its order on Microsoft's motion to dismiss, "Congress chose a broad term—facility—where it intended the statute to cover a particular function, such as internet access, as opposed to a particular piece of equipment providing that access, such as a router, laptop, or smart phone." (Dkt. 38 at 10.) Accordingly, the Court should not hesitate to hold that Cousineau's WM7 phone—which is a necessary and functional component to the transmission of Beacon and location information to/from Orion or the Camera—is a "facility" under the SCA. At the very least, there is a genuine issue of material fact on the issue to be resolved by the trier of fact.

2. Congress specifically identified RAM-stored communications as being held in "electronic storage."

Next, Microsoft contends that Cousineau's location information was not maintained in electronic storage because it supposedly was not "in the middle" of a chain of transmission. (Def. Mot. at 22 – 23.) That argument fails from the start, however, because Congress

[8] Microsoft also contends that Cousineau's phone can't be a facility because, if it were, then Microsoft would be allowed to grant third parties access to it. (Def. Mot. at 20 – 21.) Such a result, Microsoft contends, would run counter to the SCA's purpose, and therefore should be avoided. (*Id.*) Even if Microsoft's interpretation were accurate, however, such a consequence is not the result of an incorrect reading of the statute, as Microsoft suggests, but rather is the result of the fact that "technology evolves," and that "[w]hile earlier stages of technological development may have required large facilities for data storage, the draw of mobile devices is that their smaller storage space enables communication and information access regardless of the user's location." (Dkt. 38 at 11.) Thus, the unintended result that Microsoft posits would not result from an improper textual reading, but from the fact that rapid technological advancement has created a scenario that simply was not possible when the SCA was enacted—ordinary consumers can carry with them mobile computing devices that have the technological capacity and programmed functionality to act as facilities through which electronic communications services are provided.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

specifically recognized RAM as a form of electronic storage. And even if Congress hadn't, the communications Microsoft accessed were of Beacon location information, which were temporarily stored by the WM7 device to later be sent to Orion or Location Framework. When stored in RAM, then, Cousineau's location information was in temporary intermediate storage, incidental to its ultimate transmission.

The SCA defines "electronic storage" to include "*any* temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17)(A). And in passing the SCA, Congress recognized that "electronic storage" includes RAM and similar storage media. *See* S. Rep. No. 99-541, 1986 U.S.C.C.A.N. 3555, 3570 (1986) ("The term [electronic storage] covers storage within the random access memory of a computer as well as storage in any other form including storage of magnetic tapes, disks or other media."); *see also In re Google Inc. Cookie Placement Consumer Privacy Litig.*, MDL No. 12-2358-SLR, 2013 WL 5582866, at *8 (D. De. Oct. 9, 2013) (finding data stored in RAM to be in electronic storage). That inclusion makes sense, because RAM—by its nature—*only* temporarily stores information incidental to its ultimate end point, a fact that Microsoft acknowledges. (Dkt. 69 at 16:1 – 3.)

Here, Microsoft does not dispute that the location information it accessed was stored in the RAM on Cousineau's WM7 phone. This alone satisfies the SCA's "electronic storage" requirement.[9] *See* S. Rep. No. 99-541, at 3570; *see also In re Google*, 2013 WL 5582866, at *8. Even without the congressional conclusion, however, the Beacon location information here was undoubtedly, by Microsoft's design, in "electronic storage." Each time Location Framework tried to resolve the phone's location, Microsoft programmed it to look for new communications

[9] Likewise, Microsoft's implicit concession that Beacon location information are electronic communications, *see supra* § III.A.1., means, by definition, that the Beacon location information must have been "transmitted" by a system. 18 U.S.C. 2510(12). Such transmission, when coupled with the relevant data's temporary storage in RAM, fits the SCA's statutory definition of "electronic storage," even if the storage occurs *after* transmission. *See In re Google*, 2013 WL 5582866, at *8 (holding that plaintiffs' pleadings of "just-transmitted electronic communications" temporarily stored in "random access memory" satisfied the SCA's "electronic storage" requirement).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

in RAM, containing Beacon location information present at *a specific moment in time*. (*see* Dkt. 91 at ¶ 9 (stating that each time "an application sends a location request to the location framework, the framework determines what beacons it can see."); *see also* Ex. E, at 674 ("As the location of the device changes and repeated location requests are made[,] nearby tiles are prefetched from Orion and loaded into RAM as needed.").)

The temporarily stored location information either (i) in the case of Beacons "seen" by the WM7 device, fell between the Beacons themselves (e.g., the originating WiFi routers or cell towers) and their endpoints (e.g., Orion or Location Framework), or (ii) in the case of RAM-stored/tiled Beacon data, fell between Orion (where Beacons data sourced from WM7 phones would be "tiled"), the WM7 device (where certain tiles would be stored and then loaded into the device's RAM as the device's "best guess" of a user's location in the world), and Location Framework (which would access RAM-stored tiled Beacons upon a request from an application, like Camera, and compare it with Beacons "seen" by the device).[10] (Ex. C, at 652; Ex. E, at 668; Ex. D, at 721.) In either scenario, the RAM-stored Beacon data was an "electronic communication[] stored 'for a limited time' in the 'middle' of a transmission, i.e., when an electronic communication service temporarily stores a communication while waiting to deliver it." (Def. Mot. at 23 (quoting *In re DoubleClick*, 154 F. Supp. 2d at 512).)

In the face of the undisputed fact that it accessed Cousineau's Beacon location information while it was temporarily stored in RAM, Microsoft contends that that the tiled Beacon data stored in a WM7 device's RAM has already "reached [its] destination," and resides in RAM "as a resource the software can access to resolve location requests." (Def. Mot. at 24.) Microsoft's argument fails as an initial matter because the SCA does not distinguish between communications used as "resources" and communications in electronic storage, and Microsoft

[10] In reality, these two scenarios are two halves of one system, as Microsoft relied heavily on crowd sourcing to update and expand its Orion database, (Ex. F, at 693), before incorporating that crowd sourced data into tiles that could be returned to WM7 phones and be used to help resolve a WM7 phone's location (by once again comparing that tiled data to Beacons "seen" by the device).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

offers no basis for holding that stored communications cannot also be "resources" for authorized users. *See* 18 U.S.C. §§ 2510, 2701. Further, Microsoft's "RAM = endpoint" theory makes little sense because RAM, by its very nature, is an intermediate storage medium that only temporarily holds data pending its movement elsewhere—such as to permanent storage (e.g., to flash storage), or being retrieved and utilized by software. *See Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443, 448 (C.D. Cal. 2007) (rejecting defendants' argument that data in RAM was "stored" and not "subject to later access and retrieval"); *see also Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240, 1243 n.3 (3d Cir. 1983) (defining RAM as "a chip on which volatile internal memory is stored which is erased when the computer's power is turned off."). WM7's use of RAM here reinforces this fact: Microsoft programmed Location Framework (i) to load tile Beacons into RAM to be compared to "seen" Beacons (Dkt. 91 at ¶¶ 8 – 11), and (ii) to transfer certain "seen" Beacons to another RAM buffer for subsequent transmission to Orion. (Ex. E, at 678.) Microsoft's supposed distinction fails, therefore, because Congress has already defined RAM as a form of electronic storage, and the facts otherwise fit cleanly in the statutory definition.

Thus, when Microsoft accessed the Beacon and location information[11] stored in the RAM of Cousineau's WM7 phone, it accessed communications in electronic storage.

B. By accessing the Beacon location information stored in the RAM of Cousineau's WM7 phone after explicitly being denied authority to do so, Microsoft violated the SCA.

Microsoft next argues that even if the SCA applies on the facts, it did not violate the Act. In support, Microsoft believes that it cannot be liable for its software's conduct, and that it

[11] Additionally, Microsoft is wrong that it did not access "backup" data, (*see* Def. Mot. at 24), because it also programmed Location Framework to back up tile Beacon data on WM7 devices for the benefit of both its users and Microsoft, (*see* Ex. H, at 583) (email from Cristina Del Amo Casado stating that "[i]n the case of no data connection we may still have cached the last few cell/wifi requests what we call server cache or tiles that may contain the needed information."). And despite Microsoft's alarm, (*see* Def. Mot. at 24), the SCA "does not specify *whose* 'purposes of backup protection' are relevant." *Cheng v. Romo*, No. 11-cv-10007, 2013 WL 6814691, at *3 n.3 (D. Mass. Dec. 20, 2013) (emphasis in original); *see Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004) ("nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user"). Accordingly, the Beacon data stored in the WM7 server cache was held in electronic storage.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

enjoyed blanket authority to access Cousineau's phone's RAM to obtain location information. Neither argument holds up. Microsoft cannot escape liability by shifting the blame to the software it programmed, nor can it succeed on its argument that Cousineau's authorization of Microsoft to access her phone's RAM-stored location information in *some* instances deprives her of any redress for Microsoft ignoring the express and specific limitations on her authorization in others. For these reasons, Microsoft's bid at summary judgment fails.

1. Microsoft can be held liable for programming its software to access Cousineau's RAM in excess of user authorization.

Microsoft asserts that it cannot be liable because the software it programmed and distributed, rather than "Microsoft itself," accessed Cousineau's RAM and the Beacon location information residing therein. (Def. Mot. at 14.) To be clear, Microsoft doesn't debate that a defendant can violate the SCA by using software, (Def. Mot. at 16 (recognizing cases where "defendants [used] software to access . . . electronic communications)), but instead suggests that the internal workings of WM7 devices (i.e., "when the Camera app requested information from RAM on Ms. Cousineau's phone [via Location Framework]") cannot violate the Act. (Def. Mot. at 16.) The chief problem with Microsoft's position is its gloss over the facts—especially inasmuch as Microsoft used Location Framework to improve its Orion database through crowd sourcing but *chose* to limit its own ability to access users' location information *in any way* (including locally on WM7 devices themselves).

As this Court has already acknowledged, "Microsoft voluntarily limited its own authorization to access consumer data in designing and marketing [the WM7 with specific] user-controlled privacy settings." (Dkt. 38 at 12 – 13.) To that end, Microsoft, through the Camera's consent dialog box, was candid with its users about what enabling the Camera's location functionality meant—that location information would be "shar[ed]" when the "camera used [users'] location[s]." (Dkt. 65 at ¶ 4.) Early drafts of the dialog were even more candid—explaining that "***Each time* the camera accesses your location, *Microsoft* will collect**

information about your current location[.]" (Camera Experience Functional Specification, Dkt. 72-24, at 205 (emphasis added).) Microsoft itself clarified that this earlier version of the Camera location consent dialog—reflecting Microsoft's "collection" of location information—accurately describes the *same* functionality addressed by the implemented consent prompt, and makes clear that the user is being asked to share location information with Microsoft *each time* Camera was opened with location functionality enabled. (Dep. Tr. of Shamik Bandyopadhyay, Dkt. 72-25, at 49:9 – 50:23; Lydick Tr. at 48:5 – 18, 76:23 – 77:2, 91:15 – 94:11 (explaining that Camera called Location Framework every time it was opened).)

Obviously, Microsoft's "collection" of a user's location information "each time the camera access[ed a user's] location," (Dkt. 71-24, at 205), did not involve Microsoft employees arriving to retrieve it. Rather, Microsoft collected the data through its software-proxy: Location Framework. *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001) (finding that automated software's access of publicly accessible website exceeded the scope of authorized access).[12] And the first step of that collection and/or sharing was Location Framework's—and, by extension, Microsoft's—access of recent Beacon data, including both information identifying "seen" Beacons and tiled Beacon data, stored in the WM7 device's RAM.[13] Stated simply, Microsoft offered WM7 users the purported ability to limit its access to their location information, which occurred "*each time*" Camera was opened. (Lydick Tr. 48:5 – 18, 76:23 – 77:2, 91:15 – 94:11) The fact that it ignored its own self-imposed and self-described limitations

---

[12] *See also Harris v. comScore*, 292 F.R.D. 579 (N.D. Ill. 2013) (certifying class on SCA claims premised on access by Defendant's software); *Rene v. G.F. Fischers, Inc.*, 817 F. Supp. 2d 1090 (S.D. Ind. 2011) (denying motion to dismiss claim premised on defendants' use of keylogging software); *Microsoft Corp. v. John Does 1 – 82*, No. 3:13-cv-319, 2013 WL 6119242 (W.D.N.C. Nov. 21, 2013) (granting default judgment and permanent injunction where Microsoft alleged that defendants' software violated, *inter alia*, the SCA).

[13] Further, given the nature of transient storage, the "seen" Beacon data obtained by the WM7 Background Scanners (i.e., as received through each recurrent scan) must have been stored in RAM, where it is periodically refreshed and replaced, and where—upon the launching of the Camera application—it was improperly accessed by Location Framework (and Microsoft) and occasionally transmitted to Orion. (*See* Ex. C, at 650 – 52.) To the extent Microsoft contends to the contrary on reply (i.e., that information concerning "seen" Beacons was not held in RAM), no contrary evidence has been produced in discovery, thereby evincing disputed issues of material fact and rendering summary judgment on the issue improper. *See* Fed. R. Civ. P. 56(c)(1)(B).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

(i.e., assuming a user did not immediately select "allow" when presented with the dialog) shows that its routine access to location information via Location Framework was *not* authorized.

2. Cousineau authorized Microsoft to access her phone's RAM and obtain communications *only* in specific and limited instances.

Microsoft next argues that because Cousineau authorized Microsoft's access to location information in *some* instances (such as for the pre-installed Maps application), any access to location information by Location Framework—e.g., when called by Camera—was not a matter of "unauthorized access," but a matter of "misuse" of data that Microsoft already had permission to access. (Def. Mot. at 16 – 17.) Thus, Microsoft explains, the SCA applies to instances where a "trespasser gains access to information to which he is not entitled to see, not those in which the trespasser uses the information in an unauthorized way." (*Id.* at 17 (quoting *Educ. Testing Serv. v. Stanley H. Kaplan, Educ. Ctr, Ltd.*, 965 F. Supp. 731, 740 (D. Md. 1997)).) But Cousineau, through her consent choices, *only* authorized Microsoft to access her location information on discrete occasions (i.e., only at certain times and in certain locations), and Microsoft violated the SCA by accessing her RAM-stored location information in instances when and where Cousineau specifically prohibited it from doing so.

The SCA prohibits intentionally exceeding the scope of authorization to access a facility through which an ECS is provided. *See* 18 U.S.C. 2701(a)(2). Microsoft designed the WM7 system to give (or at least offer) users the ability to specifically control *when and where* Microsoft would have access to their location information (i.e., when and where it would be "shared" or "collected" by Microsoft, through Location Framework). (*See* Dkt. 65 at ¶ 4.). For her part, Cousineau authorized Microsoft to access her phone's RAM and retrieve her location information *only* in certain instances (i.e., when prompted by location-enabled applications), and specifically forbade Microsoft authority to access it in others (when requested by Camera, for instance). (*See* Dkt. 65 at ¶ 4; Dkt. 69 at 24:8 – 21.) By giving her the option of restricting its access to her locational data through the Camera, Microsoft not only defined the scope of its

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

authorization to access Cousineau's RAM-stored location information, it also gave Cousineau a "reasonable expectation of privacy" in her location information in those instances where she had denied Microsoft authority to access it.[14] (*See* Dkt. 38 at 8 n.3 (citing *United States v. Katz*, 389 U.S. 347, 352 (1967).) Thus, rather than giving Microsoft unconditional access to her RAM-stored location information (as Microsoft suggests, (Def. Mot. at 16 – 17)), Cousineau granted Microsoft—by its own design of the WM7 Camera application—authorization on a case-by-case basis. Because Cousineau specifically *denied* Microsoft access to her location information when and wherever she used her Camera application, Microsoft lacked *any* authority to access her phone's RAM-stored location information through Cousineau's use of Camera. And because it accessed it anyway (i.e., when and wherever Camera was launched), Microsoft violated the SCA. *See* 18 U.S.C. § 2710(a).

As such, Microsoft's "misuse" argument—i.e., that "the SCA forbids unauthorized *access* to communications, not unauthorized *use* of communications a defendant was authorized to access for some purposes," (Def. Mot. at 17)—misses the point. If, hypothetically, the WM7 "master location switch" was the *only* measure of control that a user had to limit Microsoft's access and/or use of location information (i.e., if Microsoft accessed/collected data when the master switch was "on" and then later used it when the switch was flipped "off"), then there would be a decent argument for misuse of location information as opposed to unauthorized access. But that's just not consistent with the design of WM7's Location Framework software (as called by Camera), which always required a fresh look at "seen" Beacons and then compared those signals to RAM-stored tiled Beacon data. (Dkt. 91 at ¶ 9.) Moreover, it ignores (i) that Cousineau alleges that Microsoft *accessed* her RAM when it was not authorized to do so—i.e., pursuant to a request from Camera—and (ii) that the SCA specifically prohibits "exceed[ing] the

[14] As noted above, this choice was important to Cousineau, who was not comfortable with providing Microsoft access to her location information while she was using Camera during her work, but didn't mind providing access when "checking in" to a restaurant on Facebook or looking up driving directions on Maps. Cousineau's ability to choose *when and where* to authorize access to her location was meaningful.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

scope of authorized access." 18 U.S.C. § 2701. If, as Microsoft seems to suggest, Cousineau didn't have the right to authorize Microsoft's access to her phone's RAM in some instances but not others, then the SCA's prohibition on exceeding the *scope* of authorized access would be meaningless.

Likewise, Microsoft's reliance on case law where defendants were given blanket authority to *access* facilities or computers but were specifically forbidden from making certain *use* of that access is misplaced. In *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (*en banc*), for example, the defendant was effectively authorized to access certain company data,[15] but was then prohibited from disclosing that same accessed information. *Id.* at 856. Here, in contrast, Microsoft lacked *any* authority to *access* Cousineau's RAM-stored location information—at all—when and where Cousineau opened Camera (even if, on different instances where Cousineau used location-enabled applications that she *had* authorized, Microsoft could access whatever data was then-stored in RAM when and where the application was used). This reading is entirely consistent with Ninth Circuit precedent, as the *Nosal* Court specifically recognized that the SCA's "exceeds the scope" language was intended to prevent "the circumvention of technological access barriers," rather than the misappropriation of information. 676 F.3d at 863. By WM7's design, Microsoft gave Cousineau the option to create a "technological access barrier"—by presenting the location consent dialog box on the first opening of the Camera application and allowing users to limit the scope of Microsoft's access to their RAM-stored location information at certain times and places—but chose to program its software to ignore and circumvent that barrier as a matter of course. As such, *Nosal* is of no help to Microsoft.

The same problem befalls Microsoft's reliance on *Educ. Testing Serv*, 965 F. Supp. 731, and *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F. Supp. 2d 817 (E.D. Mich. 2000). (Def. Mot. at 17.) Both cases note that the SCA applies where "the trespasser gains access to

[15] In *Nosal*, the defendant was charged for aiding and abetting CFAA violations, but the individuals who he aided had authorization to access the data. *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

information which he is not entitled to see, not those in which the trespasser uses the information in an unauthorized way." *Educ. Testing Serv.*, 965 F. Supp. at 740; *see also Sherman & Co.*, 94 F. Supp. 2d at 821. And despite Microsoft's attempts to recast the operation of the WM7 phone and Cousineau's allegations, this is not a case of "malicious or larcenous" misuse of access. (Def. Mot. at 17 (quoting *Sherman*, 94 F. Supp. 2d at 821).) Cousineau did not allege that, for instance, Microsoft re-appropriated and re-used data obtained during *other* location-access sessions (e.g., by saving-then-reusing location information accessed during a Facebook session) when and where Cousineau used Camera. Indeed, Location Framework worked in the opposite way, by—each and every time it was launched—accessing *unique* location information that was *then-and-there* available and visible to the device.[16]

As such, Microsoft's liability under the SCA turns entirely on its practice of accessing temporarily stored Beacon communications at specific times (i.e., when- and wherever Camera was opened) in attempts to (i) figure out where Cousineau was and (ii) potentially crowd source new Beacon data from her device for its own benefit. Thus, it doesn't matter whether "the Camera app accessed location tiles she had . . . previously authorized other Microsoft applications (such as Maps or Internet Explorer) to access."[17] (Def. Mot. at 17.) From the user's perspective, "tiled" Beacon data *only* carries significance when associated with a temporal element—i.e., *when* Beacons were "seen" by the phone, and *which* specific Beacons were in fact

---

[16] To this point, Microsoft suggests that Cousineau cannot prove her case because she cannot show that the tile data accessed by Location Framework at the times she used Camera had not been accessed previously by other applications. (Def. Mot. at 17.) That argument is defeated by the design of Microsoft's Location Framework software—which, *every* time it was invoked by Camera, would, at least, (i) initiate a *new* scan for Beacon's then-and-there visible to the phone, (Ex. C, at 652; Ex. D, at 721), and (ii) access tiled data that was marked with a unique timestamp, so that Microsoft could temporalize her phone's location. (Dkt. 64-2 at 6 (noting unique timestamp present with "tracking information . . . allowing the remote side to know at what point in time the device was at [its] location."). WM7 was not designed to "hold on to" previously accessed location information (e.g., so that Camera could bypass Location Framework entirely)—rather, it was designed to take advantage of its unrestrained access to location information at every opportunity.

[17] Of course, Microsoft's attempt to over-simplify this issue additionally ignores that Location Framework looks at *both* tiled Beacon data stored in RAM *and* Beacons "seen" by the device. (Dkt. 91 at ¶¶ 8, 10.) Both elements serve as estimates of a WM7's location in the world at a certain time—and Microsoft's access of either (both were accessed every time Camera was launched) violated the SCA.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

"seen"—rather, it accessed her *then*-stored Beacon communications in an effort to determine where she was at that point in time. Essentially, Microsoft claims that it had authority to access specific tiles, but Cousineau asserts that Microsoft went beyond that and also accessed private communications (the RAM-stored locational data) associating tile data with specific "seen" Beacons and GPS coordinates at a specific time. Stated otherwise, Microsoft was able to discern that "*this* User is within *this* bounded area, within sight of *these* Beacons, at *this* time."[18]

Thus, because Cousineau *denied* Microsoft access to her location information when and where she used Camera, Microsoft violated the SCA by accessing it anyway every time the Camera was used. (Lydick Tr. at 23:19 – 30:13, 48:5 – 18, 76:23 – 77:2, 91:15 – 94:11 (Camera called Location Framework every time it was launched, regardless of user consent choice); Del Amo Casado Tr. at 138:2 – 18 (Once called, Location Framework accessed location information because "[it] doesn't know whether the application [calling obtained] user consent."); *see also* Ex. E, at 677 (diagramming the location resolution process as beginning with a request from outside Location Framework).) By exploiting its unrestrained access to her location information, Microsoft both kept track of Cousineau's location without her consent (via Location Framework) and, by WM7's design, aggressively crowd sourced (or sought to crowd source) new Beacon information from her device whenever possible.

Thus, by accessing Cousineau's RAM to obtain location information when it was specifically denied authority to do so, Microsoft "exceeded the scope of authorized access" to her WM7 phone, obtained electronic communications in electronic storage and violated the SCA.

IV. CONCLUSION

For the reasons stated above, Plaintiff respectfully requests that this Court deny Defendant's Motion for Summary Judgment.

---

[18] Microsoft could use its same argument to claim that, because it—through the Maps application—already had access to all street information in Seattle (e.g., street names, intersections, etc.), it wouldn't matter if it collected street data regarding a user's location at given times, even if that user had denied it permission to do so (i.e., in the same way one could deny Microsoft's access to location information when Camera was used).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992

Dated: January 8, 2014

Respectfully submitted,

REBECCA COUSINEAU,
individually on her own behalf and on behalf of all others similarly situated,

By: /s/ Rafey S. Balabanian
One of Plaintiff's Attorneys

Jay Edelson (Admitted *Pro Hac Vice*)
jedelson@edelson.com
Rafey S. Balabanian (Admitted *Pro Hac Vice*)
rbalabanian@edelson.com
Benjamin S. Thomassen (Admitted *Pro Hac Vice*)
bthomassen@edelson.com
Chandler R. Givens (Admitted *Pro Hac Vice*)
cgivens@edelson.com
J. Dominick Larry (Admitted *Pro Hac Vice*)
nlarry@edelson.com
EDELSON PC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

By: /s/ Kim D. Stephens
One of Plaintiff's Attorneys

Kim D. Stephens, WSBA #11984
kstephens@tousley.com
Janissa A. Strabuk, WSBA # 21827
jstrabuk@tousley.com
TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
Tel: 206.682.5600
Fax: 206.682.2992

Counsel for Plaintiff Rebecca Cousineau and the Putative Class

CERTIFICATE OF SERVICE

I, Benjamin S. Thomassen, an attorney, hereby certify that on January 8th, 2014, I served the above and foregoing ***Plaintiff's Response in Opposition to Microsoft's Motion for Summary Judgment*** by causing true and accurate copies of such paper to be sent to all counsel of record via electronic mail.

/s/ Benjamin S. Thomassen

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL 206-682-5600 • FAX 206-682-2992